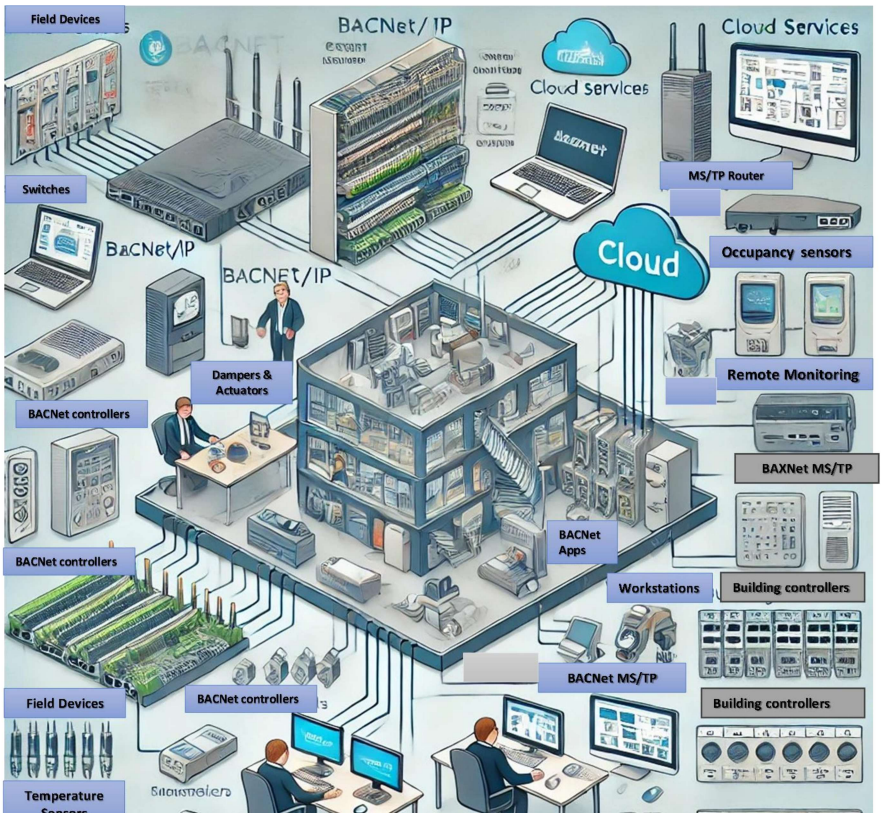
International Journal of Innovative Technology
and Creative Engineering
IJITCE (ISSN:2045-8711)
Vol.14 No.12 Dec 2024



IJITCE PUBLICATION
International Journal of Innovative Technology & Creative Engineering
Vol.14 No:12
Dec 2024

www.ijitce.co.uk

IJITCE PUBLICATION

UK: Managing Editor
International Journal of Innovative Technology and Creative Engineering
1a park lane,
Cranford
London
TW59WA
UK

USA: Editor
International Journal of Innovative Technology and Creative Engineering
Dr. Arumugam
Department of Chemistry
University of Georgia
GA-30602, USA.

India: Editor
International Journal of Innovative Technology & Creative Engineering
36/4 12th Avenue,
1 st cross St,
VaigaiColony
Ashok Nagar
Chennai, India 600083

Email: editor@ijitce.co.uk

www.ijitce.co.uk

Dear Researcher,
Greetings!

Articles in this issue discusses about:

1. Enhancing Building Automation with BACnet: A Secure and Scalable Approach
2. Side-Channel Vulnerabilities in Homomorphic encryption: Threats and Counter Measures

We look forward many newer technologies in the next month.

Thanks,

Editorial Team
IJITCE
www.ijitce.co.uk

Editorial Members

Dr. Chee Kyun Ng Ph.D
Department of Computer and Communication Systems,
Faculty of Engineering,Universiti Putra Malaysia,UPMSerdang, 43400 Selangor,Malaysia.

Dr. Simon SEE Ph.D
Chief Technologist and Technical Director at Oracle Corporation, Associate Professor (Adjunct) at Nanyang Technological University
Professor (Adjunct) at ShangaiJiaotong University, 27 West Coast Rise #08-12,Singapore 127470

Dr. sc.agr. Horst Juergen SCHWARTZ Ph.D,
Humboldt-University of Berlin,Faculty of Agriculture and Horticulture,Asternplatz 2a, D-12203 Berlin,Germany

Dr. Marco L. BianchiniPh.D
Italian National Research Council; IBAF-CNR,Via Salaria km 29.300, 00015 MonterotondoScalo (RM),Italy

Dr. NijadKabbara Ph.D
Marine Research Centre / Remote Sensing Centre/ National Council for Scientific Research,
P. O. Box: 189 Jounieh,Lebanon

Dr. Aaron Solomon Ph.D
Department of Computer Science,
National Chi Nan University,No. 303, University Road,Puli Town, Nantou County 54561,Taiwan

Dr. Arthanariee. A. M M.Sc.,M.Phil.,M.S.,Ph.D
Director - Bharathidasan School of Computer Applications, Ellispettai, Erode, Tamil Nadu,India

Dr. Takaharu KAMEOKA, Ph.D
Professor, Laboratory of Food,
Environmental & Cultural Informatics Division of Sustainable Resource Sciences,
Graduate School of Bioresources,Mie University, 1577 Kurimamachiya-cho, Tsu, Mie, 514-8507, Japan

Dr. M. Sivakumar M.C.A.,ITIL.,PRINCE2.,ISTQB.,OCP.,ICP. Ph.D.
Technology Architect, Healthcare and Insurance Industry, Chicago, USA

Dr. Bulent AcmaPh.D
Anadolu University,
Department of Economics,Unit of Southeastern Anatolia Project(GAP),26470 Eskisehir,TURKEY

Dr. Selvanathan Arumugam Ph.D
Research Scientist, Department of Chemistry, University of Georgia, GA-30602,USA.

Dr. S. Prasath Ph.D
Assistant Professor, School of Computer Science, VET Institute of Arts & Science (Co-Edu) College, Erode, Tamil Nadu, India

Dr. P.Periyasamy, M.C.A.,M.Phil.,Ph.D.
Associate Professor, Department of Computer Science and Applications, SRM Trichy Arts and Science College, SRM Nagar, Trichy - Chennai Highway, Near Samayapuram, Trichy - 621 105,

Mr. V N Prem Anand
Vice President, Cyber Society of India

Review Board Members

Dr. Rajaram Venkataraman
Chief Executive Officer, Vel Tech TBI || Convener, FICCI TN State Technology Panel || Founder, Navya Insights || President, SPIN Chennai

Dr. Paul Koltun
Senior Research ScientistLCA and Industrial Ecology Group,Metallic& Ceramic Materials,CSIRO Process Science & Engineering Private Bag 33, Clayton South MDC 3169,Gate 5 Normanby Rd., Clayton Vic. 3168, Australia

Dr. Zhiming Yang MD., Ph. D.
Department of Radiation Oncology and Molecular Radiation Science,1550 Orleans Street Rm 441, Baltimore MD, 21231,USA

Dr. Jifeng Wang
Department of Mechanical Science and Engineering, University of Illinois at Urbana-Champaign Urbana, Illinois, 61801, USA

Dr. Giuseppe Baldacchini
ENEA - Frascati Research Center, Via Enrico Fermi 45 - P.O. Box 65,00044 Frascati, Roma, ITALY.

Dr. MutamedTurkiNayefKhatib
Assistant Professor of Telecommunication Engineering,Head of Telecommunication Engineering Department,Palestine Technical University (Kadoorie), TulKarm, PALESTINE.

Dr.P.UmaMaheswari
Prof &Head,Depaartment of CSE/IT, INFO Institute of Engineering,Coimbatore.

Dr. T. Christopher, Ph.D.,
Assistant Professor &Head,Department of Computer Science,Government Arts College(Autonomous),Udumalpet, India.

Dr. T. DEVI Ph.D. Engg. (Warwick, UK),
Head,Department of Computer Applications,Bharathiar University,Coimbatore-641 046, India.

Dr. Renato J. orsato
Professor at FGV-EAESP,Getulio Vargas Foundation,São Paulo Business School,Rualtapeva, 474 (8° andar),01332-000, São Paulo (SP), Brazil Visiting Scholar at INSEAD,INSEAD Social Innovation Centre,Boulevard de Constance,77305 Fontainebleau - France

Y. BenalYurtlu
Assist. Prof. OndokuzMayis University

Dr.Sumeer Gul
Assistant Professor,Department of Library and Information Science,University of Kashmir,India

Dr. ChutimaBoonthum-Denecke, Ph.D
Department of Computer Science,Science& Technology Bldg., Rm 120,Hampton University,Hampton, VA 23688

Dr. Renato J. Orsato
Professor at FGV-EAESP,Getulio Vargas Foundation,São Paulo Business SchoolRualtapeva, 474 (8° andar),01332-000, São Paulo (SP), Brazil

Dr. Lucy M. Brown, Ph.D.
Texas State University,601 University Drive,School of Journalism and Mass Communication,OM330B,San Marcos, TX 78666

JavadRobati
Crop Production Departement,University of Maragheh,Golshahr,Maragheh,Iran

VineshSukumar (PhD, MBA)
Product Engineering Segment Manager, Imaging Products, Aptina Imaging Inc.

Dr. Binod Kumar PhD(CS), M.Phil.(CS), MIAENG,MIEEE
Professor, JSPM's Rajarshi Shahu College of Engineering, MCA Dept., Pune, India.

Dr. S. B. Warkad
Associate Professor, Department of Electrical Engineering, Priyadarshini College of Engineering, Nagpur, India

Dr. doc. Ing. RostislavChoteborský, Ph.D.
Katedramateriálu a strojírenskétechnologie Technickáfakulta,Českázemedelskáuniverzita v Praze,Kamýcká 129, Praha 6, 165 21

Dr. Paul Koltun
Senior Research ScientistLCA and Industrial Ecology Group,Metallic& Ceramic Materials,CSIRO Process Science & Engineering Private Bag 33, Clayton South MDC 3169,Gate 5 Normanby Rd., Clayton Vic. 3168

DR.ChutimaBoonthum-Denecke, Ph.D
Department of Computer Science,Science& Technology Bldg.,HamptonUniversity,Hampton, VA 23688

Mr. Abhishek Taneja B.sc(Electronics),M.B.E,M.C.A.,M.Phil.,
Assistant Professor in the Department of Computer Science & Applications, at Dronacharya Institute of Management and Technology, Kurukshetra. (India).

Dr. Ing. RostislavChotěborský,ph.d,
Katedramateriálu a strojírenskétechnologie, Technickáfakulta,Českázemědělskáuniverzita v Praze,Kamýcká 129, Praha 6, 165 21

Dr. AmalaVijayaSelvi Rajan, B.sc,Ph.d,
Faculty – Information Technology Dubai Women's College – Higher Colleges of Technology,P.O. Box – 16062, Dubai, UAE

Naik Nitin AshokraoB.sc,M.Sc
Lecturer in YeshwantMahavidyalayaNanded University

Dr.A.Kathirvell, B.E, M.E, Ph.D,MISTE, MIACSIT, MENGG
Professor - Department of Computer Science and Engineering,Tagore Engineering College, Chennai

Dr. H. S. Fadewar B.sc,M.sc,M.Phil.,ph.d,PGDBM,B.Ed.
Associate Professor - Sinhgad Institute of Management & Computer Application, Mumbai-BangloreWesternly Express Way Narhe, Pune - 41

Dr. David Batten
Leader, Algal Pre-Feasibility Study,Transport Technologies and Sustainable Fuels,CSIRO Energy Transformed Flagship Private Bag 1,Aspendale, Vic. 3195,AUSTRALIA

Dr R C Panda
(MTech& PhD(IITM);Ex-Faculty (Curtin Univ Tech, Perth, Australia))Scientist CLRI (CSIR), Adyar, Chennai - 600 020,India

Miss Jing He
PH.D. Candidate of Georgia State University,1450 Willow Lake Dr. NE,Atlanta, GA, 30329

Jeremiah Neubert
Assistant Professor,MechanicalEngineering,University of North Dakota

Hui Shen
Mechanical Engineering Dept,Ohio Northern Univ.

Dr. Xiangfa Wu, Ph.D.
Assistant Professor / Mechanical Engineering,NORTH DAKOTA STATE UNIVERSITY

SeraphinChallyAbou
Professor,Mechanical& Industrial Engineering Depart,MEHS Program, 235 Voss-Kovach Hall,1305 OrdeanCourt,Duluth, Minnesota 55812-3042

Dr. Qiang Cheng, Ph.D.
Assistant Professor,Computer Science Department Southern Illinois University CarbondaleFaner Hall, Room 2140-Mail Code 45111000 Faner Drive, Carbondale, IL 62901

Dr. Carlos Barrios, PhD
Assistant Professor of Architecture,School of Architecture and Planning,The Catholic University of America

Y. BenalYurtlu
Assist. Prof. OndokuzMayis University

Dr. Lucy M. Brown, Ph.D.
Texas State University,601 University Drive,School of Journalism and Mass Communication,OM330B,San Marcos, TX 78666

Dr. Paul Koltun
Senior Research ScientistLCA and Industrial Ecology Group,Metallic& Ceramic Materials CSIRO Process Science & Engineering

Dr.Sumeer Gul
Assistant Professor,Department of Library and Information Science,University of Kashmir,India

Dr. ChutimaBoonthum-Denecke, Ph.D
Department of Computer Science,Science& Technology Bldg., Rm 120,Hampton University,Hampton, VA 23688

Dr. Renato J. Orsato
Professor at FGV-EAESP,Getulio Vargas Foundation,São Paulo Business School,RuaItapeva, 474 (8° andar)01332-000, São Paulo (SP), Brazil

Dr. Wael M. G. Ibrahim
Department Head-Electronics Engineering Technology Dept.School of Engineering Technology ECPI College of Technology 5501 Greenwich Road - Suite 100,Virginia Beach, VA 23462

Dr. Messaoud Jake Bahoura
Associate Professor-Engineering Department and Center for Materials Research Norfolk State University,700 Park avenue,Norfolk, VA 23504

Dr. V. P. Eswaramurthy M.C.A., M.Phil., Ph.D.,
Assistant Professor of Computer Science, Government Arts College(Autonomous), Salem-636 007, India.

Dr. P. Kamakkannan,M.C.A., Ph.D .,
Assistant Professor of Computer Science, Government Arts College(Autonomous), Salem-636 007, India.

Dr. V. Karthikeyani Ph.D.,
Assistant Professor of Computer Science, Government Arts College(Autonomous), Salem-636 008, India.

Dr. K. Thangadurai Ph.D.,
Assistant Professor, Department of Computer Science, Government Arts College (Autonomous), Karur - 639 005,India.

Dr. N. Maheswari Ph.D.,
Assistant Professor, Department of MCA, Faculty of Engineering and Technology, SRM University, Kattangulathur, Kanchipiram Dt - 603 203, India.

Mr. Md. Musfique Anwar B.Sc(Engg.)
Lecturer, Computer Science & Engineering Department, Jahangirnagar University, Savar, Dhaka, Bangladesh.

Mrs. Smitha Ramachandran M.Sc(CS).,
SAP Analyst, Akzonobel, Slough, United Kingdom.

Dr. V. Vallimayil Ph.D.,
Director, Department of MCA, Vivekanandha Business School For Women, Elayampalayam, Tiruchengode - 637 205, India.

Mr. M. Moorthi M.C.A., M.Phil.,
Assistant Professor, Department of computer Applications, Kongu Arts and Science College, India

PremaSelvarajBsc,M.C.A,M.Phil
Assistant Professor,Department of Computer Science,KSR College of Arts and Science, Tiruchengode

Mr. G. Rajendran M.C.A., M.Phil., N.E.T., PGDBM., PGDBF.,
Assistant Professor, Department of Computer Science, Government Arts College, Salem, India.

Dr. Pradeep H Pendse B.E.,M.M.S.,Ph.d
Dean - IT,Welingkar Institute of Management Development and Research, Mumbai, India

Muhammad Javed
Centre for Next Generation Localisation, School of Computing, Dublin City University, Dublin 9, Ireland

Dr. G. GOBI
Assistant Professor-Department of Physics,Government Arts College,Salem - 636 007

Dr.S.Senthilkumar
Post Doctoral Research Fellow, (Mathematics and Computer Science & Applications),UniversitiSainsMalaysia,School of Mathematical Sciences, Pulau Pinang-11800,[PENANG],MALAYSIA.

Manoj Sharma
Associate Professor Deptt. of ECE, PrannathParnami Institute of Management & Technology, Hissar, Haryana, India

RAMKUMAR JAGANATHAN
Asst-Professor,Dept of Computer Science, V.L.B Janakiammal college of Arts & Science, Coimbatore,TamilNadu, India

Dr. S. B. Warkad
Assoc. Professor, Priyadarshini College of Engineering, Nagpur, Maharashtra State, India

Dr. Saurabh Pal
Associate Professor, UNS Institute of Engg. & Tech., VBS Purvanchal University, Jaunpur, India

Manimala
Assistant Professor, Department of Applied Electronics and Instrumentation, St Joseph's College of Engineering & Technology, Choondacherry Post, Kottayam Dt. Kerala -686579

Dr. Qazi S. M. Zia-ul-Haque
Control Engineer Synchrotron-light for Experimental Sciences and Applications in the Middle East (SESAME),P. O. Box 7, Allan 19252, Jordan

Dr. A. Subramani, M.C.A.,M.Phil.,Ph.D.
Professor,Department of Computer Applications, K.S.R. College of Engineering, Tiruchengode - 637215

Dr. SeraphinChallyAbou
Professor, Mechanical & Industrial Engineering Depart. MEHS Program, 235 Voss-Kovach Hall, 1305 Ordean Court Duluth, Minnesota 55812-3042

Dr. K. Kousalya
Professor, Department of CSE,Kongu Engineering College,Perundurai-638 052

Dr. (Mrs.) R. Uma Rani
Asso.Prof., Department of Computer Science, Sri Sarada College For Women, Salem-16, Tamil Nadu, India.

MOHAMMAD YAZDANI-ASRAMI
Electrical and Computer Engineering Department, Babol"Noshirvani" University of Technology, Iran.

Dr. Kulasekharan, N, Ph.D
Technical Lead - CFD,GE Appliances and Lighting,
GE India,John F Welch Technology Center,Plot # 122, EPIP, Phase 2,Whitefield Road,Bangalore – 560066, India.

Dr. Manjeet Bansal
Dean (Post Graduate),Department of Civil Engineering,Punjab Technical University,GianiZail Singh Campus,Bathinda -151001 (Punjab),INDIA

Dr. Oliver Jukić
Vice Dean for education,Virovitica College,MatijeGupca 78,33000 Virovitica, Croatia

Dr. Lori A. Wolff, Ph.D., J.D.
Professor of Leadership and Counselor Education, The University of Mississippi,Department of Leadership and Counselor Education, 139 Guyton University, MS 38677

Contents

1. Enhancing Building Automation with BACnet: A Secure and scalable approach……..1663
2. Exploring Side-Channel Vulnerabilities in Homomorphic Encryption: Threats and countermeasures……..1678

Enhancing Building Automation with BACnet: A Secure and Scalable Approach

Premanand Narasimhan
Director, Techiespeaks OPC Pvt Ltd,
Independent Researcher/Consultant
Vice President, Cyber Society of India
premvn@gmail.com

Dr.N.Kala
Assistant Professor, Former Director i/c,
Centre for Cyber Forensics and Information Security,
University of Madras,
Chennai, Tamil Nadu,
Kalabaskar@gmail.com

Abstract

Building Automation and Control Network (BACnet) is a standardized communicationrotocol designed to enable interoperability between various building automation systems (BAS), including HVAC (Heating, Ventilation, and Air Conditioning), lighting, security, fire safety, and energy management. Developed and maintained by ASHRAE as an open protocol under ISO 16484-5, BACnet facilitates seamless communication between devices from different manufacturers, promoting cost-effective and scalable automation solutions. The protocol operates using an object-oriented model and supports multiple transport mechanisms such as BACnet/IP, Ethernet, MS/TP, and LonTalk. As smart buildings and IoT-driven Infrastructures expand, BACnet remains a cornerstone in energy-efficient and sustainable building management. However, security concerns have prompted the development of BACnet Secure Connect (BACnet/SC) to address cyber vulnerabilities. This paper provides a comprehensive overview of BACnet, its architecture, key functionalities, applications, and security considerations, with references

drawn from books, journals, blogs, official reports, and online educational resources.

Introduction

The increasing demand for energy efficiency, operational cost reduction, and seamless automation in modern buildings has driven the adoption of intelligent building management systems (BMS). BACnet, an open-standard protocol developed by the American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE), plays a crucial role in integrating and optimizing building automation systems (BAS). It enables multiple subsystems, such as HVAC, lighting, security, fire safety, and energy management, to communicate efficiently without proprietary restrictions.

BACnet's object-oriented structure allows different devices to exchange data using standardized services, ensuring interoperability across manufacturers. It supports multiple transport mechanisms, including Ethernet, BACnet/IP, MS/TP (Master-Slave/Token-Passing), PTP (Point-to-Point), and LonTalk, allowing flexibility in deployment across small and large-scale facilities.

With the rise of smart buildings and Internet of Things (IoT) applications, BACnet has gained significant importance in modern infrastructure. However, the protocol's original design lacked robust security features, making it susceptible to cyber threats such as unauthorized access and data tampering. The introduction of BACnet Secure Connect (BACnet/SC) addresses these vulnerabilities by providing encryption and authentication mechanisms.

This paper explores the fundamentals of BACnet, including its key features, communication model, applications, and security challenges. The discussion will be supported by references from books, peer-reviewed journals, industry blogs, YouTube technical presentations, government and private-sector reports, and Open Educational Resources (OERs).

Background information

what is BACnet?

BACnet (Building Automation and Control Network) is a data communication protocol specifically designed for building automation and control systems. It enables devices from different manufacturers to communicate with each other seamlessly in a building's infrastructure.

Key Features

1. Standardized Protocol: BACnet is an open, international standard (ISO 16484-5) developed and maintained by ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers).
2. Interoperability: It allows integration between HVAC (Heating, Ventilation, and Air Conditioning), lighting, access control, fire safety, and other systems in a building.
3. Vendor Neutral: Since it's open-source, manufacturers can implement it without licensing restrictions.
4. Scalability: It supports simple to complex systems, making it ideal for small buildings or large campuses.

How BACnet Works?

- Object-Oriented: BACnet uses "objects" to represent various devices or functions, like sensors, actuators, or alarms.
- Services: Devices interact using services such as *read*, *write*, *subscribe*, and *acknowledge*.
- Communication Protocols: BACnet works over:
  - Ethernet
  - IP (BACnet/IP)
  - MS/TP (Master-Slave/Token-Passing)
  - LonTalk
  - PTP (Point-to-Point)

Common Uses

- HVAC Control: Managing heating, cooling, and ventilation systems.
- Lighting Systems: Automated lighting controls.
- Access Control: Integration with security systems.
- Energy Management: Monitoring and optimizing energy consumption.
- Fire & Safety Systems: Communication for alarms and emergency systems.

Benefits of BACnet

1. Cost-Effective: Reduces integration costs with a standardized protocol.
2. Flexibility: Easily expand or modify systems with BACnet-compatible devices.
3. Simplified Integration: Multi-vendor devices can work together seamlessly.

BACnet is a cornerstone technology for smart buildings and IoT-enabled infrastructure, driving energy efficiency and building automation.

Industries Leading BACnet/SC Adoption

BACnet/SC (Secure Connect) adoption is being driven by industries that require robust cybersecurity, operational reliability, and compliance with security

standards. The following industries are at the forefront of BACnet/SC implementation:

1. Healthcare Facilities

- Why: Hospitals and clinics rely on BACnet systems to manage critical infrastructure, including HVAC, fire alarms, and lighting. Cyberattacks on these systems can endanger patient safety.
- **BACnet/SC Adoption**:
  - Ensures secure communication and prevents unauthorized access to life-critical systems.
  - Meets regulatory requirements like HIPAA (Health Insurance Portability and Accountability Act) and other healthcare cybersecurity mandates.
- Example Use Cases:
  - Securing patient ward HVAC controls.
  - Ensuring fire safety and access systems remain tamper-proof.

2. Data Centers

- Why: Data centers require precision cooling, power management, and environmental controls to ensure 24/7 availability. Any unauthorized changes can disrupt operations, leading to financial losses.
- BACnet/SC Adoption:
  - Encrypts communication to prevent malicious tampering with HVAC and power systems.
  - Enables secure remote management of data center BAS infrastructure.
- Example Use Cases:
  - Protecting cooling systems from attacks that could overheat servers.
  - Securing environmental monitoring against unauthorized changes.

4. Smart Buildings and Commercial Real Estate

- Why: Large office buildings, retail spaces, and smart campuses increasingly integrate IoT devices, increasing the attack surface.
- BACnet/SC Adoption:
  - Mitigates risks from open BACnet/IP protocols.
  - Ensures secure integration of BAS with IoT solutions (e.g., lighting, HVAC, security systems).
- Example Use Cases:
  - Preventing unauthorized manipulation of lighting systems.
  - Securing remote access for facility managers.

5. Airports and Transportation Hubs

- Why: Airports manage large-scale BAS systems, including HVAC, access control, lighting, and security, which are vulnerable to cyber-physical attacks.
- BACnet/SC Adoption:

  - Protects against Denial of Service (DoS) and Man-in-the-Middle (MitM) attacks targeting BAS systems.
  - Supports encrypted communication for secure operations.
- Example Use Cases:
  - Securing fire safety and ventilation systems.
  - Preventing unauthorized changes to passenger access systems.

6. Industrial and Manufacturing Facilities

- Why: Factories, plants, and warehouses rely on BACnet to control environmental systems and integrate OT and IT networks.
- BACnet/SC Adoption:
  - Prevents operational disruptions caused by malware or ransomware targeting BAS.
  - Encrypts communication between OT devices and reduces the risk of unauthorized reconfigurations.
- Example Use Cases:
  - Protecting cleanroom environments in pharmaceutical manufacturing.
  - Preventing malicious shutdowns of industrial ventilation systems.

7. Government and Defense Facilities

Why**:** Government buildings and military bases manage secure access, HVAC, and security systems through BACnet.

- BACnet/SC Adoption:
  - Ensures compliance with cybersecurity frameworks like NIST SP 800-82.
  - Encrypts communication to protect against cyber espionage and tampering.
- Example Use Cases:
  - Securing access control systems in high-security zones.
  - Protecting HVAC systems against targeted disruptions.

7. Education Campuses

- Why: Universities and school districts use BACnet for energy management, security systems, and smart building operations.
- BACnet/SC Adoption:
  - Prevents unauthorized access to BAS systems that could compromise campus safety.
  - Supports secure integration of IoT-based learning and energy efficiency tools.
- Example Use Cases:
  - Securing lighting systems in lecture halls.

- Monitoring and protecting HVAC systems in dormitories.

How AI Automates BACnet Security?

AI improves BACnet security by enabling real-time monitoring, anomaly detection, and automated threat responses. AI-driven tools are capable of managing BACnet's complex traffic and addressing security gaps effectively.

1. AI for Real-Time Traffic Monitoring

- AI tools analyze BACnet/IP traffic in real-time and create a baseline of normal behavior.
- AI detects anomalies that deviate from the baseline, such as:
  - Excessive Who-Is or I-Am messages (indicative of reconnaissance or flooding).
  - Unauthorized WriteProperty or ReinitializeDevice commands.
  - Rogue devices broadcasting unexpected traffic.

Example Tools:

- Darktrace: Detects deviations in BACnet traffic patterns using unsupervised learning.
- Nozomi Networks Guardian: Monitors BACnet/IP traffic for anomalies and threat indicators.

2. AI-Driven Threat Intelligence

- AI tools aggregate global threat intelligence feeds (e.g., AlienVault OTX, MITRE ATT&CK) and correlate them with BACnet network activity.
- Predicts vulnerabilities in outdated firmware, device misconfigurations, or insecure communication.

Example Tools:

- Palo Alto Cortex XDR: Integrates AI with threat intelligence to identify BACnet vulnerabilities.
- IBM Watson Security: AI-powered threat detection and prediction.

3. Automated Incident Response

- AI automates responses to detected anomalies, significantly reducing response times.
- Example automated actions:
  - Isolating rogue devices sending malicious commands.
  - Blocking excessive Who-Is requests to mitigate DoS attacks.
  - Rolling back malicious configuration changes on HVAC or lighting systems.

Example Tools:

- Splunk SOAR: Automates security workflows and incident responses.
- Microsoft Defender for IoT: Identifies and blocks malicious BACnet traffic.

4. Predictive Vulnerability Detection

- AI models analyze logs and configurations to predict potential vulnerabilities or failures in BACnet devices.

- AI performs proactive scans to identify:
    - Devices running outdated firmware.
    - Weak authentication mechanisms or default credentials.

Example Tools:

- Qualys: Predictive vulnerability management for BACnet systems.
- Darktrace PREVENT: Identifies and mitigates potential weak points in OT networks.

5. Deep Packet Inspection (DPI) with AI

- AI-powered deep packet inspection (DPI) tools analyze BACnet/IP packets for protocol-specific threats.
- Identifies malformed packets, unauthorized traffic, and potential exploits.

Example Tools:

- Cisco Cyber Vision: Performs DPI for OT systems, including BACnet/IP traffic.
- Claroty xDome: Uses AI to inspect traffic for malicious BACnet packets.

Summary Table: AI in BACnet Security

AI Function	Use Case	Tools
Anomaly Detection	Detect abnormal traffic patterns	Darktrace, Nozomi Networks
Threat Intelligence	Correlate threats with BACnet traffic	Cortex XDR, IBM Watson Security
Incident Response Automation	Automate mitigation actions	Splunk SOAR, Microsoft Defender
Vulnerability Detection	Predict firmware or protocol weaknesses	Qualys, Darktrace PREVENT
Deep Packet Inspection	Inspect BACnet packets for exploits	Cisco Cyber Vision, Claroty xDome

Enhancements:

1. Security Considerations – While BACnet is highly interoperable, cybersecurity has become a significant concern. BACnet Secure Connect (BACnet/SC) addresses these security challenges by providing encrypted communications.
2. Industry Adoption – Mentioning industries that commonly use BACnet (e.g., commercial buildings, healthcare facilities, data centers, smart cities) can highlight its broad adoption.
3. Comparison with Other Protocols – A brief comparison with protocols like Modbus, KNX, and LonWorks can add depth.
4. Use Case Example – A real-world example of BACnet integration in a large facility can make it more relatable.

1. Security Considerations in BACnet

While BACnet offers interoperability and scalability, its original design lacked strong security measures, making it vulnerable to cyber threats such as unauthorized access, data interception, and malware attacks. As buildings become increasingly interconnected through IoT devices and cloud-based solutions, securing BACnet-based automation systems is a priority.

1.1 Common Security Risks in BACnet

- Lack of Encryption: Older BACnet implementations transmit data in plaintext, making it susceptible to interception and modification.
- Weak Authentication Mechanisms: Without strong authentication, unauthorized devices can access the network and manipulate building systems.
- Denial of Service (DoS) Attacks: Attackers can flood BACnet networks with excessive traffic, disrupting building operations.
- Lateral Movement in Networks: If a BACnet device is compromised, attackers can use it as a gateway to infiltrate other connected systems.

1.2 BACnet Secure Connect (BACnet/SC)

To address these challenges, BACnet Secure Connect (BACnet/SC) was

introduced as a secure extension of BACnet. It provides:

- TLS Encryption: Implements Transport Layer Security (TLS) to encrypt communication, preventing unauthorized interception.
- **Certificate-based Authentication:**
- Devices require valid certificates to establish connections, reducing unauthorized access risks.
- Firewall-Friendly Communication: BACnet/SC operates over WebSockets, making it compatible with existing IT security policies.
- Backward Compatibility: It allows integration with traditional BACnet networks, enabling gradual adoption without a complete overhaul.

2. Industry Adoption of BACnet

BACnet is widely adopted in several industries due to its open standard and flexibility. Below are key sectors where BACnet plays a crucial role:

2.1 Commercial Buildings & Smart Offices

- Used for integrating HVAC, lighting, and energy management to optimize resource usage and reduce costs.
- Facilitates demand-response strategies where buildings adjust energy consumption based on utility signals.

2.2 Healthcare Facilities

- Ensures climate-controlled environments in operating rooms and pharmaceutical storage.
- Integrates with fire alarm systems to automatically adjust airflow during emergencies.

2.3 Data Center's

- Used for monitoring temperature, humidity, and cooling efficiency.
- Helps prevent overheating and optimizes power usage.

2.4 Industrial & Manufacturing Facilities

- Enables real-time monitoring of ventilation and air quality.
- Used in hazardous environment monitoring, ensuring compliance with safety regulations.

2.5 Airports & Transportation Hubs

- Automates lighting and security systems for efficient energy savings.

- Integrates access control for secure zone management.

2.6 Government & Military Buildings

- Helps manage energy efficiency initiatives in public sector buildings.
- Enhances security through integrated access control systems.

3. Bacnet Protocols

Brief Overview of BACnet Protocols

BACnet (Building Automation and Control Network) is a standardized communication protocol developed to enable interoperability between building automation devices. It provides a structured method for devices such as HVAC systems, lighting, fire alarms, and access control to exchange data. BACnet operates using several transport mechanisms, each suited for different applications and network requirements.

1. BACnet Protocol Stack and Object-Oriented Model

BACnet follows a layered architecture similar to the OSI model, where each layer defines how messages are structured, transmitted, and processed. It uses an object-oriented approach, meaning devices and functions (such as sensors, actuators, and controllers) are represented as objects with specific properties and behaviors.

2. BACnet Transport Protocols

BACnet supports multiple network transport options, allowing flexibility in deployment across different building sizes and infrastructures.

2.1 BACnet/IP (Internet Protocol)

- Uses standard Ethernet and TCP/IP networks for communication.
- Allows seamless integration with IT infrastructure and cloud-based solutions.
- Supports BACnet Secure Connect (BACnet/SC) for enhanced cybersecurity.
- Ideal for large-scale building automation systems with remote access.

2.2 BACnet MS/TP (Master-Slave/Token-Passing)

- A serial communication protocol designed for low-cost, low-speed field devices.

- Operates over RS-485 with a master-slave token-passing mechanism.

2.3 BACnet Ethernet (ISO 8802-3) Uses Ethernet MAC addresses for device communication.

- Faster than MS/TP but lacks IP level routing capabilities.
- Best suited for LAN-based building automation systems.

2.4 BACnet PTP (Point-to-Point)

- A direct serial connection protocol for two BACnet devices.
- Used in small- to medium-sized buildings where Ethernet/IP is unnecessary.
- More cost-effective but slower than BACnet/IP.

Uses RS-232 or modems for remote monitoring applications. BACnet Protocol	Best for	Speed	Security	se Case
BACnet/ IP	Large buildings IT-integrated BMS	High	High (TLS with BACnet/ SC)	Smart buildings, cloud-connected automation
BACnet MS/TP	Small/ medium buildings	Moderate	Low	HVAC, simple lighting control
BACnet Ethernet	LAN-based systems	High	Medium	High-speed automation in industrial settings
BACnet PTP	Remote or legacy systems	Low	Low	Dial-up or point-to-point monitoring
BACnet LonTalk	Specialized networks	Moderate	Low	Older LonWorks-based systems
BACnet/SC	Secure cloud integration	High	Very High	Critical infrastructure, financial & government buildings

- Used in legacy systems for remote device
- Communication over dial-up.

2.5 BACnet LonTalk

- Supports Echelon's LonWorks protocol.
- Enables communication over twisted-pair, powerline, fiber, and wireless media.
- Less commonly used today due to the dominance of BACnet/IP.

2.6 BACnet Secure Connect (BACnet/SC)

- Introduced to enhance cybersecurity in BACnet networks.
- Uses TLS encryption and certificate-based authentication.
- Operates over WebSockets, making it compatible with firewalls and modern IT security standards.
- Ensures secure and encrypted communication between BACnet devices.

3. BACnet Communication Services

BACnet devices interact using standardized services that facilitate data exchange. These include:

- Read Property & Write Property – Retrieve or modify data from a device.
- Subscribe & Confirmed COV (Change of Value) – Notify systems of data changes in real-time.
- Alarm & Event Notification – Alert operators of anomalies or system failures.
- Device Management Services – Identify, synchronize, or restart devices.

4. Choosing the Right BACnet Protocol

The selection of a BACnet transport protocol depends on network size, cost, speed, and security requirements:

BACnet's flexibility in communication protocols makes it a widely adopted standard for building automation. The transition towards BACnet/IP and BACnet Secure Connect (BACnet/SC) is shaping the future of smart buildings by enhancing integration with IoT, cloud computing, and cybersecurity standards.

4. Comparison with Other Building Automation Protocols

BACnet is not the only protocol used in building automation. Below is a comparison with other widely used protocols:

Feature	BACnet	Modbus	KNX	LonWorks
Standardization	ISO 16484-5	Open Standard	ISO/IEC 14543-3	ANSI/EIA 709.1
Primary Use Case	Building automation	Industrial Automation	Smart homes / buildings	Commercial automation
Interoperability	High	Limited	High	High
Security Features	BACnet/SC (TLS)	Basic Authentication	Encrypted Communication	Encrypted Communication
Communication Layers	Ethernet, IP, MS/TP, LonTalk, PTP	RS-485, TCP/IP	Ethernet, Twisted Pair, RF	Ethernet, Powerline, RF
Scalability	High	Moderate	High	High

Key Takeaways

- BACnet is ideal for large-scale building automation, particularly in commercial and industrial settings.
- Modbus is best suited for industrial control systems (ICS) but lacks interoperability across vendors.
- KNX is widely used in home automation and smart buildings with strong encryption features.
- LonWorks offers similar interoperability to BACnet but is less widely adopted.

4. Real-World Use Case: BACnet in Smart City Infrastructure

A real-world example can help demonstrate BACnet's impact in building automation.

Case Study: BACnet Deployment in a Smart City Project

Project: Smart Building Automation in Singapore's Marina Bay Sands

- Challenge: Managing HVAC, lighting, and fire safety across a vast, energy-intensive environment.
- Solution: Implementing BACnet-enabled building management systems for seamless communication across different vendors' devices.
- Outcome:
    - 20% reduction in energy costs through automated lighting and HVAC control.
    - Enhanced fire safety via real-time sensor monitoring and automated emergency responses.

- Scalable expansion without vendor lock-in, ensuring long-term adaptability.

Case Study: BACnet in Healthcare

Project: Hospital Automation in Cleveland Clinic

- Challenge: Ensuring precise temperature and humidity control in operating rooms and patient care areas.
- Solution: BACnet-based automation for real-time HVAC monitoring and air quality control.
- Outcome:
  - Improved patient safety by maintaining sterile environments.
  - Automated alerts for potential failures, reducing maintenance costs.
  - Optimized energy efficiency, leading to $300,000 in annual energy savings.

Conclusion

BACnet has revolutionized building automation by providing a standardized communication protocol that enhances interoperability, scalability, and cost-efficiency. While it has faced cybersecurity challenges, the introduction of BACnet Secure Connect (BACnet/SC) has significantly improved security by implementing TLS encryption and authentication mechanisms. The widespread adoption of BACnet in commercial buildings, healthcare, data center's, and smart cities highlights its role in driving energy-efficient and intelligent infrastructure. As the demand for IoT-integrated smart buildings continues to rise, BACnet will remain a cornerstone technology in the evolution of building automation.

Industries such as healthcare, data centers, smart buildings, and industrial facilities lead the adoption of BACnet/SC due to their need for secure, reliable building automation. AI tools such as Darktrace, Nozomi Networks Guardian, and Microsoft Defender for IoT are revolutionizing BACnet security by enabling real-time anomaly detection, predictive vulnerability analysis, and automated responses. Through advanced monitoring, AI ensures that BACnet systems remain resilient against modern cyber threats while enhancing operational efficiency.

References

1. **Books**
   - Newman, M. (2013). *Direct Digital Control: A Guide to Distributed Building Automation*. CRC Press.
   - Barney, G. C. (2016). *Intelligent Building Systems: Principles and Applications*. Routledge.

2. **Journals**
   - Wang, S., & Xie, J. (2013). "Integrating Building Automation Systems with BACnet." *Automation in Construction*, 30, 107-116.
   - Rios, R., & Lopes, S. (2021). "Cybersecurity Risks in BACnet-based Building Automation Systems." *Journal of Building Engineering*, 35, 102089.
3. **Blogs & Online Articles**
   - ASHRAE (2023). "BACnet Overview and Future Developments." Retrieved from www.ashrae.org
   - Building Automation Monthly (2023). "Understanding BACnet and its Role in Smart Buildings." Retrieved from www.buildingautomationmonthly.com
4. **YouTube Technical Videos**
   - "BACnet Explained: A Beginner's Guide" – YouTube, 2023
   - "BACnet Secure Connect and Cybersecurity" – YouTube, 2024
5. **Government and Private Reports**
   - National Institute of Standards and Technology (NIST). (2022). *Guide to Securing Building Automation Systems*.
   - U.S. Department of Energy (DOE). (2021). *Smart Buildings: The Role of BACnet in Energy Management*.
6. **Open Educational Resources (OERs)**
   - Massachusetts Institute of Technology (MIT) OpenCourseWare: *Building Automation and Control Systems*.
   - OpenLearn (2023). "Energy-Efficient Smart Buildings and BACnet."

Exploring Side-Channel Vulnerabilities in Homomorphic Encryption: Threats and Countermeasures

Farheen
Student
Masters in Cyber Forensics and Information Security,
Centre for Cyber Forensics and Information Security,
University of Madras, Chennai - 600005
farheen.unom@gmail.com

Premanand Narasimhan
Director, Techiespeaks OPC Pvt Ltd
Independent Researcher/Consultant
Vice President Cyber Society of India
premvn@gmail.com

Dr.N.Kala
Assistant Professor
Former Director i/c
Centre for Cyber Forensics and Information Security
University of Madras,
Chennai – 600005
kalabaskar@gmail.com

Abstract

Homomorphic encryption (HE) allows for numeric data to be manipulated without decrypting the data and the need for encryption keys, preserving privacy in sensitive applications. However, it is possible to break homomorphic encryption using side-channel attacks, which exploit physical or behavioral leakages caused during data transmission. This paper explores these vulnerabilities in homomorphic encryption highlighting critical vulnerabilities in popular HE libraries. Furthermore, this paper will also analyze the effectiveness of existing countermeasures, and propose strategies to enhance HE resilience against such attacks. The findings aim to bridge the gap between theoretical HE security and its practical implementation, fostering robust cryptographic systems in real-world applications.

Keywords: Homomorphic Encryption (HE), Side-Channel Attacks (SCA), Cryptographic vulnerabilities, Data Masking, Timing Attacks, Threat Analysis

Introduction

Homomorphic encryption (HE) is a transformative cryptographic technique that permits computations on encrypted numeric data without decryption, thereby preserving data confidentiality throughout processing. This capability is particularly advantageous in scenarios where sensitive information must be processed in untrusted environments, such as cloud computing and outsourced data services.

Despite HE's robust theoretical security foundations, practical implementations are susceptible to side-channel attacks, exploits that leverage unintended information leakage from cryptographic systems' physical implementations. These attacks can extract sensitive information by analyzing various physical parameters, including power

consumption, electromagnetic emissions, and execution timing.

Recent studies have highlighted the vulnerability of HE schemes to such attacks. Aydin et al. demonstrated that the Microsoft SEAL HE library is prone to side-channel attacks and is capable of extracting encryption keys during the key generation phase by exploiting leakage in the number theoretic transform algorithm. Similarly, another study revealed that power-based side-channel attacks could extract entire plaintext messages from SEAL's encryption phase with a single power measurement. These findings underscore the critical need to analyze and mitigate side-channel vulnerabilities in HE systems to ensure their security in real-world applications.

This paper aims to:

- Explore the susceptibility of homomorphic encryption (HE) schemes to side-channel attacks, providing a comprehensive analysis of potential threats.
- Evaluate existing countermeasures to determine their effectiveness in mitigating these vulnerabilities.
- Propose strategies to enhance the resilience of HE implementations against side-channel attacks, bridging the gap between theoretical security and practical deployment.

By addressing these objectives, we contribute to the development of more secure cryptographic systems suitable for deployment in diverse and potentially adversarial environments.

1. Literature Review

A series of works by Aydin et al. (2020, 2021) have demonstrated several vulnerabilities in the Microsoft SEAL HE library, one of the most widely used libraries for homomorphic encryption. In their paper *Leaking Secrets in Homomorphic Encryption with Side-Channel Attacks*, the authors highlighted how side-channel leakages could allow attackers to extract plaintext messages from encrypted data by analyzing device-side encryption operations. The study emphasized that the encryption operations in SEAL could inadvertently reveal valuable information, making the system susceptible to various forms of SCAs (Aydin et al., 2020).

A subsequent study by Aydin et al., *Exposing Side-Channel Leakage of SEAL Homomorphic Encryption Library*, further investigated the vulnerabilities of SEAL, revealing a new side-channel leakage in which attackers could exploit ternary values leaked during computations. This vulnerability posed a direct threat to the confidentiality of encrypted data, urging the need for countermeasures to mitigate such risks (Aydin et al., 2021).

In another paper, *Single-Trace Side-Channel Leakage of the SEAL Homomorphic Encryption Library*, the authors demonstrated the effectiveness of a side-channel attack on SEAL, which could extract plaintext messages using just a single trace of side-channel information. This work introduced a new level of complexity in side-channel attacks, suggesting that even minimal data leakage could lead to the recovery of sensitive information, further emphasising the vulnerability of HE libraries to SCAs (Aydin et al., 2020).

Finally, the study *Characterizing Memory Side Channels in HE Applications* by Pal et al. (2022) [2] explored the impact of memory access patterns in Fully Homomorphic

Encryption (FHE) applications. The authors found that variations in memory access could unintentionally expose sensitive information during computations. They proposed mitigation strategies, such as memory access masking, to reduce the risk of such side-channel leaks, highlighting the ongoing need for effective countermeasures to secure HE systems against SCAs

2. Preliminaries

In this section, we provide foundational concepts essential for understanding the subsequent discussions on homomorphic encryption, side-channel attacks, and the vulnerabilities arising from their intersection.

2.1 Homomorphic Encryption

Homomorphic encryption (HE) is a cryptographic technique that permits computations to be performed directly on encrypted data without requiring decryption. The result of such computations, when decrypted, yields the same outcome as if the operations were performed on the plaintext. This property is invaluable for preserving data privacy during processing.

2.1.1 Mathematical Foundation

A homomorphic encryption scheme is defined by a tuple of algorithms:

2. **Key Generation (KeyGen):** Produces a public and private key pair.
3. **Encryption (Enc):** Converts plaintext data into ciphertext using the public key.
4. **Decryption (Dec):** Recovers the plaintext from ciphertext using the private key.
5. **Evaluation (Eval):** Performs specific operations on ciphertexts, resulting in a new ciphertext that corresponds to the operation applied to the underlying plaintexts.

Formally, for a given operation ◦ \circ◦ and plaintexts m1m_1m1 and m2m_2m2 :

$$Dec(Eval(Enc(m1),Enc(m2)))=m1 \circ m2 \text{Dec}(\text{Eval}(\text{Enc}(m_1), \text{Enc}(m_2))) = m_1 \circ m_2 Dec(Eval(Enc(m1),Enc(m2)))=m1 ◦ m2$$

This equation ensures that operations on encrypted data are consistent with those on plaintexts.

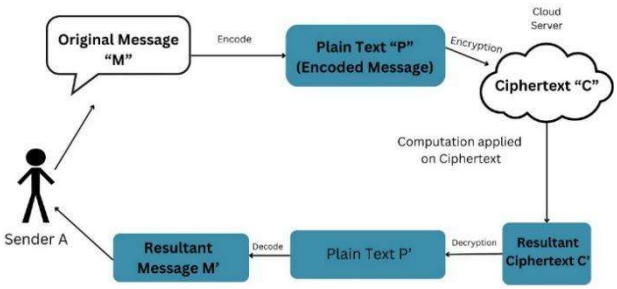


Figure 1: Homomorphic Encryption Architecture Diagram

2.1.2 Types of Homomorphic Encryption

- **Partially Homomorphic Encryption (PHE):** Supports a single type of operation (either addition or multiplication) on ciphertexts.
- **Somewhat Homomorphic Encryption (SHE):** Allows a limited number of both addition and multiplication operations.
- **Fully Homomorphic Encryption (FHE):** Enables arbitrary computations, including any number of additions and multiplications, on ciphertexts.

2.2 Side-Channel Attacks

Side-channel attacks (SCAs) exploit unintended information leakage from the

physical implementation of cryptographic systems. Instead of targeting theoretical weaknesses in algorithms, SCAs leverage observable phenomena such as timing information, power consumption, electromagnetic emissions, or acoustic signals to infer sensitive data.

2.2.1 Common Types of Side-Channel Attacks

- **Timing Attacks:** Analyze the time taken to execute cryptographic algorithms to deduce information about the secret keys.
- **Power Analysis Attacks:** Monitor power consumption patterns during cryptographic operations to extract secret information.
- **Electromagnetic Attacks:** Measure electromagnetic emissions from devices during computation to gather confidential data.
- **Acoustic Cryptanalysis:** Utilize sounds produced by hardware components during processing to retrieve sensitive information.

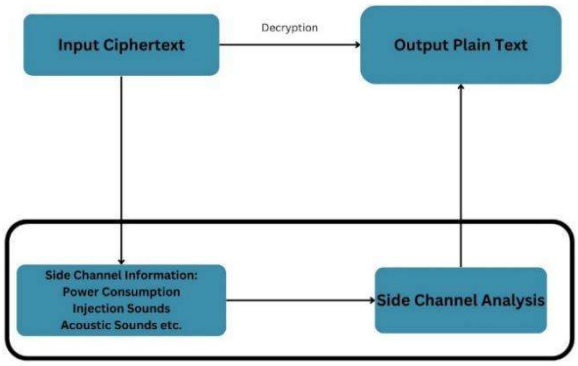


Figure 2: Side Channel Attack

2.3 Homomorphic Encryption Vulnerabilities to Side-Channel Attacks

While homomorphic encryption schemes are theoretically designed to be secure, their practical implementations can be susceptible to side-channel attacks. The complexity of HE operations often results in prolonged computation times and increased power consumption, providing a larger surface for SCAs. For instance, during the evaluation phase, variations in power usage or execution time can inadvertently leak information about the processed ciphertexts, potentially allowing attackers to reconstruct the underlying plaintexts or even recover secret keys.

Understanding these foundational concepts is crucial for analyzing the security of homomorphic encryption systems and developing effective countermeasures against side-channel attacks.

3. Side Channel Vulnerability Threats in Homomorphic Encryption

3.1 Types of Side-Channel Attacks in Homomorphic Encryption

SCAs leverage observable characteristics such as timing information, power consumption, or electromagnetic emissions to infer sensitive information. In the context of HE, these attacks can be particularly concerning:

- **Timing Attacks**: Variations in execution time during HE operations can reveal information about the processed data.
- **Power Analysis Attacks**: Monitoring power consumption patterns during HE computations can lead to the extraction of secret keys or plaintexts.
- **Electromagnetic Attacks**: Electromagnetic emissions during HE operations can be analyzed to uncover confidential information.

3.2 Documented Vulnerabilities

Recent studies have highlighted specific vulnerabilities in HE implementations:

- **Microsoft SEAL Library**: Research demonstrated that side-channel leakages in the Microsoft SEAL HE

- library could be exploited to steal encryption keys during the key generation phase. The attack abuses leakage in the number theoretic transform (NTT) algorithm, which is integral to the library's operations.

- **Single-Trace Attacks**: Another study revealed that single-trace side-channel attacks could extract entire plaintext messages from the SEAL library's encryption phase with just one power measurement, showcasing the feasibility of such attacks in real-world scenarios.

3.3 Threats in HE aiding to side-channel attacks

3.3.1. Side-Channel Attacks (SCAs)

- Side-channel attacks exploit unintended leakage from physical implementations of cryptographic algorithms, such as timing variations, power consumption, or electromagnetic emissions during computations.
- **Example**: Single-trace power analysis attacks can extract plaintexts or encryption keys from HE schemes, such as Microsoft SEAL, by analyzing power consumption during encryption or evaluation phases.
- **Impact**: SCAs bypass theoretical security guarantees, leaking sensitive information without directly attacking the cryptographic algorithms.

3.3.2. Implementation Bugs

- Errors in implementing HE schemes, such as flawed arithmetic or insecure library usage, can introduce exploitable vulnerabilities.
- **Example**: Incorrect parameter settings in fully homomorphic encryption (HE) schemes may lead to ciphertext malleability or reduced security levels.
- **Impact**: Implementation bugs can compromise cryptographic guarantees and expose data to unauthorized access.

3.3.3 Parameter Misconfiguration

HE schemes rely on secure parameter settings, such as key size, noise levels, and ciphertext modulus. Incorrect configurations can undermine security.

- **Example**: Choosing a low noise budget in HE schemes may result in decryption errors or easier attacks by adversaries.
- **Impact**: Inadequate parameter selection compromises both functionality and security.

3.3.4. Resource Exhaustion Attacks

- HE operations are computationally intensive, and attackers can exploit this to execute denial-of-service (DoS) attacks.
- **Example**: Sending repeated requests for complex HE evaluations can overload system resources.
- **Impact**: Such attacks disrupt system availability, particularly in cloud-based HE implementations.

3.3.5. Data Leakage During Operations

Intermediate data generated during HE operations may unintentionally reveal information about the encrypted data.

- **Example**: Bootstrapping (a noise-reduction operation in HE) can potentially leak sensitive information if not securely implemented.

- **Impact**: Leaked intermediate values undermine data confidentiality.

- **3.3.6. Chosen-Ciphertext Attacks (CCA)**

In chosen-ciphertext attacks, adversaries manipulate ciphertexts to infer information about the plaintext or encryption keys.

- **Example**: Modifying ciphertexts and observing the decryption effects can help attackers reconstruct sensitive data.
- **Impact**: Improper validation or padding mechanisms in HE implementations can make them susceptible to CCA.

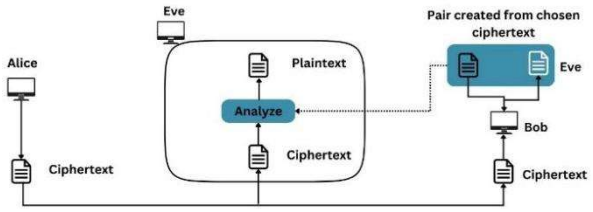


Figure 3: Chosen Ciphertext Attack

3.3.7. Cross-Platform Vulnerabilities

- Variations in hardware or software platforms introduce unique vulnerabilities in HE systems.
- **Example**: An HE library optimized for one hardware may leak side-channel information when deployed on less secure devices.
- **Impact**: Platform-specific weaknesses provide attackers with unexpected attack vectors.

3.3.8. Key Management Challenges

Secure generation, storage, and distribution of HE keys are critical. Improper key management practices can result in unauthorized access.

- **Example**: Exposing private keys in shared environments can compromise encrypted data for multiple users.
- **Impact**: Poor key management directly undermines HE system security.

3.3.9. Quantum Threats

Future advancements in quantum computing pose a significant threat to HE schemes.

- **Example**: Shor's algorithm could break cryptographic primitives based on integer factorization or discrete logarithms.
- **Impact**: The confidentiality of encrypted data may not be guaranteed in a post-quantum era.

4. Countermeasures To Combat Side Channel Threats In Homomorphic Encryption

To address the vulnerabilities associated with homomorphic encryption (HE), several countermeasures have been proposed and implemented. These measures focus on enhancing the security and resilience of HE systems against known threats, ensuring both theoretical robustness and practical applicability.

Below are the key countermeasures:

4.1. Mitigating Side-Channel Attacks (SCAs)

- **Constant-Time Implementations**: Design algorithms to execute in constant time, independent of input values, to prevent timing-based leakages.
- **Power and Electromagnetic Analysis Resistance**: Employ masking techniques or hardware shields to obscure power consumption and electromagnetic emissions.
- **Secure Hardware Environments**: Deploy HE computations on tamper-resistant hardware or trusted execution environments (TEEs) to reduce susceptibility to SCAs.

4.2. Preventing Implementation Bugs

- **Rigorous Testing**: Conduct extensive testing of HE implementations using both automated and manual methods to identify and rectify potential flaws.
- **Formal Verification**: Apply formal methods to verify the correctness of HE algorithms and their implementation.
- **Library Security Audits**: Perform regular audits of HE libraries to ensure compliance with secure coding practices.

4.3. Ensuring Proper Parameter Configuration

- **Guidelines for Parameter Selection**: Follow established standards, such as those outlined by NIST or HomomorphicEncryption.org, to choose secure and optimal parameters.
- **Dynamic Parameter Adjustment**: Implement adaptive systems to monitor and adjust parameters based on the computational context and noise levels.

4.4. Preventing Resource Exhaustion Attacks

- **Rate Limiting**: Limit the number of HE operations a system can perform within a specific timeframe to prevent overload.
- **Efficient Algorithms**: Optimize HE algorithms to reduce computational overhead and mitigate susceptibility to denial-of-service (DoS) attacks.
- **Cloud-Based Load Balancing**: Use load-balancing techniques in cloud-based HE systems to distribute computational tasks and avoid resource bottlenecks.

4.5. Preventing Data Leakage During Operations

- **Secure Bootstrapping**: Employ advanced bootstrapping techniques that minimize leakage, such as noise-hiding mechanisms or encryption masking.
- **Randomized Processing**: Introduce randomness into intermediate computations to obscure patterns that could reveal information.

4.6. Mitigating Chosen-Ciphertext Attacks (CCA)

- **Robust Padding Schemes**: Use strong padding schemes, such as Optimal Asymmetric Encryption Padding (OAEP), to prevent ciphertext manipulation.
- **Validation of Inputs**: Ensure strict validation of ciphertexts before processing to detect and reject **malformed inputs.**
- **Authenticated Encryption**: Combine HE with authenticated encryption to detect and prevent unauthorized ciphertext alterations.

4.7. Addressing Cross-Platform Vulnerabilities

- **Platform-Specific Optimization**: Tailor HE implementations for specific hardware platforms to ensure security across varying architectures.
- **Secure Deployment Guidelines**: Provide clear instructions for deploying HE libraries securely on diverse platforms.

4.8. Strengthening Key Management

- **Secure Key Storage**: Use hardware security modules (HSMs) or secure enclaves to store keys safely.
- **Robust Key Exchange Protocols**: Implement secure key exchange mechanisms, such as Diffie-Hellman or post-quantum cryptographic methods, to protect key transmission.

- **Periodic Key Rotation**: Regularly update and rotate encryption keys to reduce the risk of compromise.

4.9. Preparing for Quantum Threats

- **Post-Quantum Cryptography Integration**: Transition to HE schemes that rely on quantum-resistant assumptions, such as lattice-based cryptography.
- **Hybrid Cryptographic Solutions**: Combine HE with classical and post-quantum algorithms to ensure long-term data confidentiality.
- **Continuous Monitoring of Quantum Advancements**: Monitor developments in quantum computing to proactively update HE systems against emerging threats.

6. Conclusion

Homomorphic encryption (HE) presents a powerful tool for secure data processing, particularly in cloud computing and privacy-preserving applications. However, as the literature demonstrates, the security of HE systems is not immune to side-channel attacks (SCAs). Research has uncovered various vulnerabilities in widely used HE libraries, such as Microsoft SEAL, revealing that attackers can exploit side-channel leakages to extract sensitive information, including plaintext data and secret keys. These vulnerabilities are significant as they can undermine the privacy guarantees provided by HE, especially in real-world scenarios where attackers may have access to physical devices or computational traces.

The studies reviewed in this paper highlight the importance of addressing side-channel risks in HE systems. While existing work has identified several forms of side-channel leakages, including those related to power consumption, timing variations, and memory access patterns, there remains a need for more robust countermeasures. Techniques such as constant-time implementations, noise injection, and memory access masking show promise in mitigating these threats, but there is still much work to be done to achieve a comprehensive and efficient defence strategy.

As HE continues to evolve, researchers must focus on developing secure and efficient implementations that can withstand side-channel attacks without sacrificing performance. Future research should explore novel techniques to enhance the resilience of HE against SCAs, ensuring its practical adoption in sensitive and privacy-critical applications. Moreover, standardization of security measures across different HE implementations will play a key role in ensuring the consistent protection of encrypted data in the face of emerging attack vectors.

In conclusion, while homomorphic encryption remains a promising cryptographic tool, its security must be strengthened against side-channel threats to guarantee its effectiveness in safeguarding data privacy.

References

Books and Journal Articles:

1. **"Cryptographic Engineering" by Çetin Kaya Koç**: This book provides an in-depth exploration of cryptographic algorithms and their implementations, including discussions on side-channel attacks and defenses.

2. **"Leaking Secrets in Homomorphic Encryption with Side-Channel Attacks" by Furkan Aydin and Aydin Aysu**: Published in the *Journal of Cryptographic Engineering*, this article demonstrates side-channel leakages in the Microsoft SEAL homomorphic encryption library, highlighting

vulnerabilities during the key generation phase.

3. **"Exposing Side-Channel Leakage of SEAL Homomorphic Encryption Library" by Furkan Aydin et al.**: This paper reveals new side-channel leakages in the Microsoft SEAL library, focusing on vulnerabilities that could be exploited to extract sensitive information.

YouTube Videos:

4. **"Single-Trace Side-Channel Attack on SEAL Homomorphic Encryption Library"**: In this talk, Furkan Aydin discusses the first side-channel attack on homomorphic encryption, demonstrating how power analysis can be used to extract plaintext from encrypted data.
5. **"Hardware Security Tutorial - Part 4 - Side Channel Attacks"**: Presented by Prof. Todd Austin from the University of Michigan, this tutorial provides an overview of side-channel attacks, including those relevant to cryptographic implementations

Blogs and Online Articles:

6. **"Homomorphic Encryption Targeted by a New Side-Channel Attack Campaign"**: This article discusses recent research demonstrating that even advanced encryption methods like homomorphic encryption are susceptible to side-channel attacks, emphasizing the need for robust security measures.

7. **"Researchers Demonstrate They Can Steal Data During Homomorphic Encryption"**: This blog post highlights vulnerabilities in homomorphic encryption that could allow attackers to extract data during the encryption process, underscoring the importance of implementing effective countermeasures.

Government and Private Reports:

8. **"Lifting the Veil on Homomorphic Encryption" by the Office of the Privacy Commissioner of Canada**: This report provides an overview of homomorphic encryption, its benefits, and potential vulnerabilities, including discussions on.

9. **"Toward Scalable Fully Homomorphic Encryption Through Light Trusted Computing Assistance"**: This research paper explores enhancing the scalability of fully homomorphic encryption by integrating trusted computing technologies, addressing performance and security challenges.

10. Aydin, Furkan & Aysu, Aydin. (2022). Exposing Side-Channel Leakage of SEAL Homomorphic Encryption Library. 10.1145/3560834.3563833.

11. Pal, A., Swaminathan, K., Pal, S., & San Miguel, J. Characterizing Memory Side Channels in FHE Applications.

12. F. Aydin, E. Karabulut, S. Potluri, E. Alkim and A. Aysu, "RevEAL: Single-Trace Side-Channel Leakage of the SEAL Homomorphic Encryption Library," 2022 Design, Automation & Test in Europe Conference & Exhibition (DATE), Antwerp, Belgium, 2022, pp. 1527-1532, doi: 10.23919/DATE54114.2022.9774724.

13. Marcolla, Chiara & Sucasas, Victor & Manzano, Marc & Bassoli, Riccardo &

Fitzek, Frank & Aaraj, Najwa. (2022). Survey on Fully Homomorphic Encryption, Theory, and Applications. Proceedings of the IEEE. PP. 1-38. 10.1109/JPROC.2022.3205665.

Academic and Conference Papers

Zhao, F., Wang, X. S., et al. (2020)
"Cryptanalysis of Machine Learning with Homomorphic Encryption and Applications to Medical Data Privacy"
In *USENIX Security Symposium*
https://www.usenix.org/conference/usenixsecurity20

Zhang, Z., Wang, X., & Wang, C. (2021)
"Side-Channel Vulnerabilities in Fully Homomorphic Encryption Libraries"
In *Proceedings of the 2021 ACM Workshop on Privacy in the Electronic Society (WPES)*
DOI: 10.1145/3471984.3473042

Chen, Y., et al. (2017)
"Side-channel leakage in matrix multiplication and its implication for lattice-based cryptography"
In *ACM CCS*
DOI: 10.1145/3133956.3134092

Liu, S., Wang, H., et al. (2016)
"A survey on side-channel attacks and countermeasures"
Journal of Cryptographic Engineering, 8(4), 315–339
DOI: 10.1007/s13389-016-0122-0

Yonetani, R., et al. (2021)
"Cache Side-channel Attacks and Countermeasures in FHE"
In *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*
IEEE Xplore

Gentry, C. (2009)
"Fully Homomorphic Encryption Using Ideal Lattices"
Ph.D. Thesis, Stanford University
https://crypto.stanford.edu/craig

Smart, N., & Vercauteren, F. (2014)
"Fully Homomorphic SIMD Operations"
In *Designs, Codes and Cryptography*
Also available in the Springer book *Homomorphic Encryption and Applications*, 2014.

Bhasin, S., & Regazzoni, F. (Eds.) (2019)
"Hardware Side-Channel Attacks: Experimental Analysis of Real Devices"
Springer International Publishing.
ISBN: 978-3-030-30618-7

Alkim, E., Bindel, N., et al. (2020)
"A New Hope: Efficient Post-Quantum Key Exchange"
USENIX Security
Discusses masking and side-channel resistance for lattice-based crypto.

Bayrak, A. G., Regazzoni, F., et al. (2013)
"Spook: Side-channel protection through obscurity"
In *ACM/IEEE DAC*
DOI: 10.1145/2463209.2488764

Chari, S., Rao, J. R., & Rohatgi, P. (2002)
"Template Attacks"
In *CHES 2002: Cryptographic Hardware and Embedded Systems*
Lecture Notes in Computer Science, Springer.

Schindler, W. (2009)
"A Timing Attack against RSA with the Chinese Remainder Theorem"
In *Cryptographic Hardware and Embedded Systems – CHES 2000*

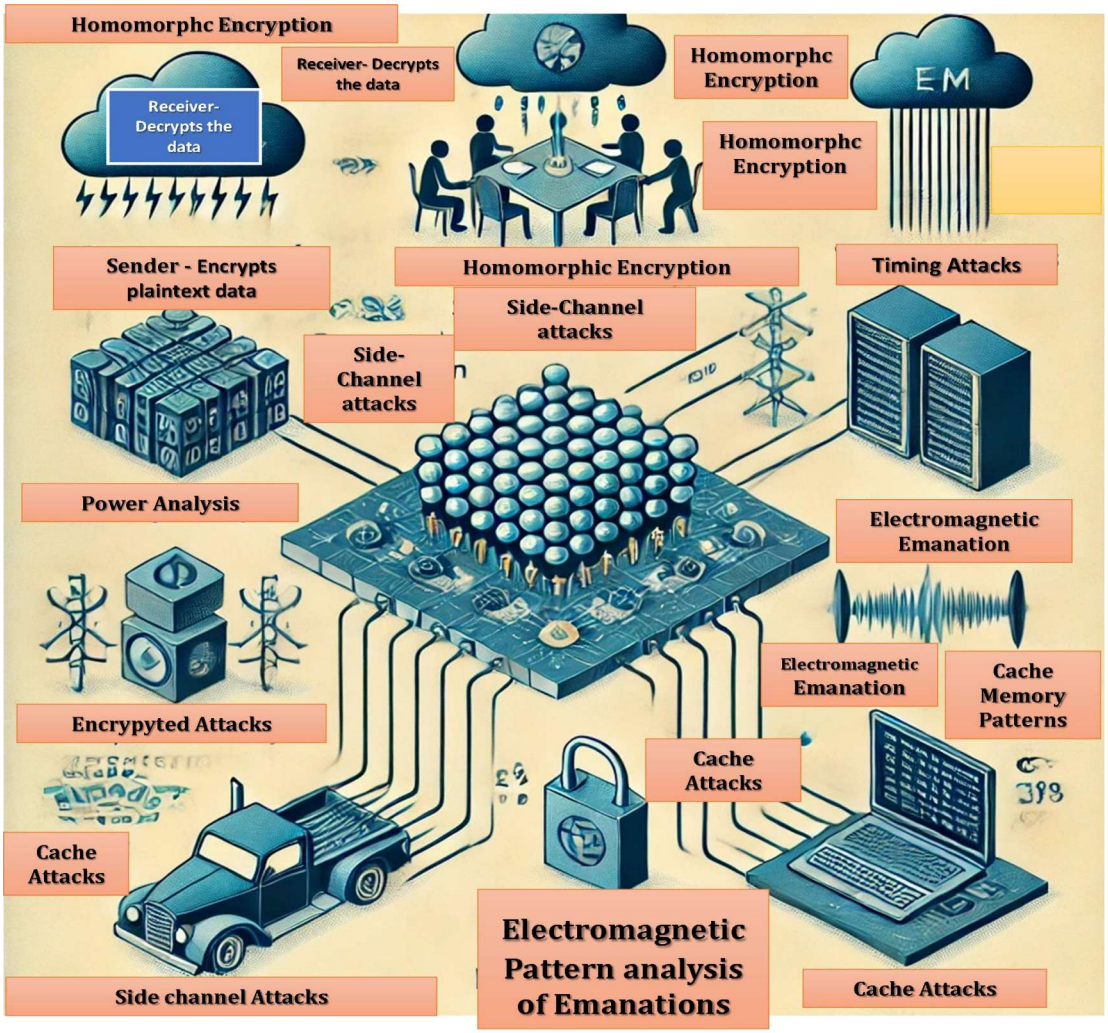
Suggestions for Practical Exploration

Review the Microsoft SEAL library and its security notes

https://github.com/microsoft/SEAL

- Explore **PALISADE** and **HElib** to test side-channel protections
https://palisade-crypto.org
https://github.com/homenc/HElib

Check out **OpenFHE**, the open-source successor to PALISADE, with improved FHE APIs
https://openfhe.org


Homomorphc Encryption
Receiver- Decrypts the data
Receiver- Decrypts the data
Homomorphc Encryption
EM
Homomorphc Encryption
Sender - Encrypts plaintext data
Homomorphic Encryption
Timing Attacks
Side-Channel attacks
Side-Channel attacks
Power Analysis
Electromagnetic Emanation
Electromagnetic Emanation
Cache Memory Patterns
Encrypyted Attacks
Cache Attacks
Cache Attacks
Electromagnetic Pattern analysis of Emanations
Side channel Attacks
Cache Attacks